

AMENDMENTS TO THE DRAWINGS

FIGURE 7 has been amended to correct some typographical errors.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

REMARKS

Claims 1-5 are pending in the above-identified application. The Office Action mailed May 2, 2007, rejected Claims 1-5 and objected to informalities in the Specification. Appropriate corrections have been made to the Specification.

Claims 1-5 are rejected under 35 U.S.C. § 101 because the claimed invention allegedly is directed to non-statutory subject matter.

Claims 1-5 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,188,369, to Ho et al. (hereinafter "Ho").

Dependent Claims 6-20 are newly added. With this response, Claims 1-20 are pending in the application.

Pursuant to 37 C.F.R. § 1.111, and for the reasons set forth below, applicants respectfully request reconsideration and allowance of the pending claims. Prior to presenting the reasons why the applicants believe that the pending claims are in condition for allowance, a brief summary of the disclosed subject matter and brief descriptions of the teachings of the cited references are provided. These summaries, however, are presented solely to assist the Examiner in recognizing the differences between the pending claims and the cited references, and should not be construed as limiting on the disclosed subject matter.

Disclosed Subject Matter

The present application discloses systems and methods for detecting malware among executable scripts. Unlike executable code, scripts are typically executed in an interpretive environment and are not compiled down to source code. Moreover, scripts are typically editable using a variety of word processing programs. Since scripts are interpreted (instead of compiled) they can be easily yet superficially modified without changing the underlying instruction. For

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

example, a variable "vName" could easily be renamed "xyzzy" throughout the body of a script without changing the functionality of the script in the least.

Malware is often detected by generating a hash of a document and checking the hash against those of known malware. In order to ensure that a legitimate file is not mistakenly identified as malware, a typical hash generation process is highly sensitive to the actual contents of the document. Unfortunately, malware designers are aware of this and have turned to modifying their malware in superficial manners to avoid detection. As indicated above, scripts can be easily modified, modified to a great degree, without changing the underlying functionality. To resolve this, the present application discloses a normalization process that generates a normalized signature for a given script and compares the normalized signature against similarly normalized signatures of known malware to determine whether the given script is malware.

The normalization process takes tokens from a script and translates them into normalized tokens according to a common naming format. For example, as recited in the specification, the variable "vName" may be translated to "V1." Routines are similarly translated to a common naming format. Additionally, non-functional statements, sometimes called no-op statements, are eliminated from the normalized signature.

When an ideal match between a normalized signature for a given script and the normalized signatures in the malware signature store is not found, a second normalized signature is generated. This second normalizing process recognizes that some statements within a script can be reordered without modifying the underlying functionality of the script. The second normalizing and comparison step addresses this. The second normalized signature removes ordinal values from the normalized tokens. For example, a first normalized token "V1" would be twice normalized simply to "V". Routine tokens are also similarly twice normalized. The result (such as shown in FIGURE 11,) is a significantly simplified set of tokens which form the second

normalized signature. The second normalized signature is then compared to twice normalized signatures of known malware. If a complete match is found on the second normalized signature, the script is reported as being malware. If a partial match is found, a report is made that the script may be malware – leaving it to the user to determine additional actions to be taken, if any.

U.S. Patent No. 7,188,369, to Ho et al. ("Ho")

Ho discloses an antivirus system having a virtual processor and plug-in capabilities. The Ho system includes an antivirus database having signatures of known viruses. The processor can receive instructions external to the system for execution in scanning for viruses. Using the signatures, and the internal and external instructions, the Ho system scans files (including generating signatures and comparing those signatures to known virus signatures in the antivirus database) to determine whether the files are/contain viruses.

While Ho discloses a particular antivirus system, and suggests that viruses may be identified by their signatures, yet Ho fails to disclose normalizing script to generate normalized signatures (as disclosed in the present application) and comparing a normalized signature to similarly normalized signatures of known malware. Further still, Ho fails to disclose twice normalizing a script and comparing the twice normalized signature of that script to twice normalized signatures of known malware in an effort to identify whether the script is or contains malware.

Specification Objections

The Office Action objected to various citations in the specification, most of which were made with regard to a trademarked name. Applicants have amended the specification to address these objections. Applicants further submit that each reference to a trademarked name is capitalized, and that each is accompanied with generic terminology.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESSTM
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Applicants believe that the causes of the objections have been fully satisfied, and request that the objections be withdrawn.

35 U.S.C. § 101 Rejections

The Office Action rejected Claims 1-5 under 35 U.S.C. § 101 as being directed to non-functional descriptive material. Applicants have amended the independent claims (Claims 1, 3, 4, and 5) to recite reporting the results of determining whether the script in question is malware. Applicants submit that reporting the results of the determination satisfies the requirements of "use, concrete, and tangible" results as required under 35 U.S.C. § 101. Accordingly, applicants request that the 35 U.S.C. § 101 rejections of Claims 1-5 be withdrawn, and the claims allowed.

35 U.S.C. § 102(e) Rejections

The Office Action rejected Claims 1-5 under 35 U.S.C. § 102(e) as being anticipated by Ho. For the reasons set forth below, applicants respectfully traverse the rejections and submit that Ho fails to disclose each and every element of Claims 1-5.

Claim 1

Applicants submit that Ho fails to disclose the following elements as recited in Claim 1:

a malware signature store including at least one known malware script signature, **wherein each malware signature in the malware signature stored is a normalized signature of a known malware script;** and

a normalization module that obtains an executable script and **generates a normalized signature for the executable script, wherein generating a normalized signature for the executable script comprises translating tokens from the executable script into normalized tokens conforming to a common format.** (Emphasis added.)

While Ho describes an antivirus database that holds a plurality of virus signatures, nothing in Ho describes or suggests that the signatures in the database have been normalized, i.e., where tokens are translated to a common naming structure suitable for comparison to other

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESSTM
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

normalized signatures. This is especially the case as the claim itself recites that generating a normalized signature **"comprises translating tokens from the executable script into normalized tokens conforming to a common format."**

As recited above, normalizing tokens in a script enable the system to compare the underlying structure of a script to normalized signatures (underlying structure) of known malware, looking beyond superficial renaming of tokens. Applicants submit that Ho fails to disclose such normalized signatures, as well as normalizing the script for comparison to normalized signatures of known malware

For the reasons set forth above, applicants submit that Ho fails to disclose each element of Claim 1. Accordingly, applicants request that the 35 U.S.C. § 102(c) rejection of this claim be withdrawn and the claim allowed.

Claim 2

Applicants submit that dependent Claim 2 is allowable for the same reasons as set forth above. Accordingly, applicants request that the 35 U.S.C. § 102(c) rejection of this claim be withdrawn and the claim allowed.

Claims 3-5

While differing in scope, applicants point out that independent Claims 3-5 recite similar subject matter to that described in independent Claim 1. In particular, Claim 3 recites:

a malware signature storage means including at least one known malware signature, **wherein each malware signature in the malware signature store means is a normalized signature of a known malware script;** and
a normalization means that obtains an executable script and **generates a normalized signature for the executable script, wherein the normalized signature for the executable script comprises a set of normalized tokens translated from corresponding tokens in the executable script into a common format suitable for comparison with the at least one malware signature in the malware signature store means;**

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESSTM
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Claim 4 recites:

generating a first normalized signature for the executable script, wherein **the first normalized signature comprises normalized tokens translated from corresponding tokens in the executable script in a format suitable for comparison to normalized signatures of known malware;** and

Claim 5 recites:

generating a first normalized signature for the executable script, wherein **the first normalized signature comprises normalized tokens translated from corresponding functional contents of the executable script in a format suitable for comparison to normalized signatures of known malware.**

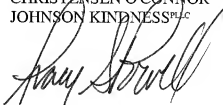
As can be seen from above, these independent claims recite elements (particularly normalizing the executable script) that are not found in Ho. Accordingly, applicants request that the 35 U.S.C. § 102(e) rejections of these claims be withdrawn and the claims allowed.

CONCLUSION

In view of the above remarks, applicants respectfully submit that the present application is in condition for allowance. Reconsideration and reexamination of the application, and allowance of the claims at an early date, are solicited. If the Examiner has any questions or comments concerning the foregoing response, the Examiner is invited to contact the applicants' undersigned attorney at the number below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLC}



Tracy S. Powell
Registration No. 53,479
Direct Dial No. 206.695.1786

TSP:laI

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100